6450-01-P

This document is scheduled to be published in the Federal Register on 11/24/2021 and available online at **federalregister.gov/d/2021-25669**, and on **govinfo.gov**

DEPARTMENT OF ENERGY

Request for Information on DOE's Cybersecurity Capability Maturity Model (C2M2) Version 2.0 (July 2021)

AGENCY: Office of Cybersecurity, Energy Security, and Emergency Response; Department of Energy.

ACTION: Request for information.

SUMMARY: In July 2021, the Department of Energy (DOE) released Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2), a tool that helps organizations evaluate and improve their cybersecurity capabilities, considering their specific risk environment. The update was guided by input from the Energy Sector C2M2 Working Group, which comprises 145 energy sector cybersecurity practitioners representing 77 energy sector and cybersecurity organizations. Version 2.0 updates the model from Version 1.1, released in 2014, and includes a variety of updates to the model domains and practices to better address emerging technologies and the evolving cyber threat landscape. Since the release in July, DOE has piloted the updated model with energy companies and utilities. To obtain the broadest possible input, DOE seeks public comment on the C2M2 to inform the C2M2 Working Group as it develops future model updates.

DATES: Comments and information must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: To access and review the Cybersecurity Capability Maturity Model (C2M2), visit *www.energy.gov/c2m2*.

Comments should be submitted by email to *C2M2@hq.doe.gov* using the Comment Submission Form available here: *https://energy.gov/sites/default/files/2021-11/Comment%20Submission%20Form%20-%20Cybersecurity%20Capability%20Maturity%20Model%20%28C2M2%29.docx*. Use the email subject line: "C2M2 Public Comment from [name/organization]."

Although DOE has routinely accepted public comment submissions through a variety of mechanisms, including postal mail and hand delivery/courier, the Department has found it necessary to make temporary modifications to the comment submission process in light of the ongoing coronavirus 2019 ("COVID-19") pandemic. DOE is currently suspending receipt of public comments via postal mail and hand delivery/courier. If a commenter finds that this change poses an undue hardship, please contact CESER staff at (202) 586-3057 to discuss the need for alternative arrangements. Once the COVID-19 pandemic health emergency is resolved, DOE anticipates resuming all of its regular options for public comment submission, including postal mail and hand delivery/courier.

FOR FURTHER INFORMATION CONTACT: Mr. Fowad Muneer, Acting Deputy Assistant Secretary for the Cybersecurity for Energy Delivery Systems Division, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. Tel.: (202) 586-5961. Email: *fowad.muneer@hq.doe.gov*.

SUPPLEMENTARY INFORMATION:

The C2M2 helps organizations evaluate and improve their cybersecurity capabilities, considering their specific risk environment. The model is a voluntary tool, tailored specifically for the energy industry, that enables companies to set targets, evaluate and benchmark their cybersecurity capabilities, and use the results to prioritize actions and investments. It is scalable

for a company of any size, and is designed to evaluate practice in both the information technology (IT) and operational technology (OT) environments.

DOE originally developed the C2M2 with input from energy industry partners in 2012, and released an updated Version 1.1 in 2014, with separate versions targeted for the electricity and oil and natural gas subsectors. Version 2.0, released July 2021, is designed for use across the energy sector, and can be used by other critical infrastructure sectors as well.

The Version 2.0 update was guided by input from the Energy Sector C2M2 Working Group, which DOE formed with the Electricity and Oil & National Gas Subsector Coordinating Councils. The update better addresses new technologies like cloud, mobile, and artificial intelligence, and evolving threats such as ransomware and supply chain risks.

While the structure of the model remains the same, this update resulted in some key changes:

- Revisions to two-thirds of model practices—including substantive changes and clarifications—along with additions, deletions, and combining of practices
- Addition of a Cybersecurity Architecture domain focused on planning, designing, and managing the cybersecurity control environment
- Significant updates to the Risk Management domain to incorporate leading risk management practices and enhance coordination between cyber and enterprise risk management
- Refresh of the Dependencies domain, now called the Third-Party Risk Management domain, to ensure the model effectively addresses third-party IT and OT cybersecurity risks, like sensitive data in the cloud and vendors with privileged access, as well as build supply chain security into organizational culture

- Integration of Information Sharing domain activities into the Threat and Vulnerability Management and Situational Awareness domains
- Addition of help text for each practice to improve clarity and consistency in how practices are applied

DOE requests public comment on the C2M2 to inform the C2M2 Working Group as it develops future model updates. Specifically, DOE seeks input on the following items:

- The usefulness of C2M2 practices in evaluating and improving cybersecurity program capabilities
- The applicability of practice language to the IT and OT environments in use by energy sector organizations
- The readability of and ability to understand practice language
- The completeness of cybersecurity domains, objectives, and practices included within the C2M2
- The effectiveness of guidance documentation (e.g., model introduction sections, domain introductions, and appendices) in conveying model concepts, architecture, and how to use the model
- Any other potential improvements to the C2M2 documentation or practices contained therein

For more information on the C2M2, or to review the model document, visit *www.energy.gov/c2m2*.

Confidential Business Information: Pursuant to 10 CFR 1004.11, any person submitting information that he or she believes to be confidential and exempt by law from public disclosure should submit via email two well-marked copies: one copy of the document marked

"confidential" including all the information believed to be confidential, and one copy of the document marked "non-confidential" with the information believed to be confidential deleted. DOE will make its own determination about the confidential status of the information and treat it according to its determination.

Signing Authority

This document of the Department of Energy was signed on November 18, 2021, by Fowad Muneer, Acting Deputy Assistant Secretary for the Cybersecurity for Energy Delivery Systems Division, pursuant to delegated authority from the Secretary of Energy. That document with the original signature and date is maintained by DOE. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned DOE Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Energy. This administrative process in no way alters the legal effect of this document upon publication in the *Federal Register*.

Signed in Washington, DC, on November 19, 2021.

_____

Treena V. Garrett,
Federal Register Liaison Officer,
U.S. Department of Energy.

[FR Doc. 2021-25669 Filed: 11/23/2021 8:45 am; Publication Date: 11/24/2021]